BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 1517 /QĐ-BTTTT	*Hà Nội, ngày 06 tháng 10 năm 2021*

QUYẾT ĐỊNH
Ban hành Yêu cầu kỹ thuật cơ bản đối với sản phẩm Nền tảng tri thức mối đe dọa an toàn thông tin

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Theo đề nghị của Cục trưởng Cục An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Yêu cầu kỹ thuật cơ bản đối với sản phẩm Nền tảng tri thức mối đe dọa an toàn thông tin (Threat Intelligence Platform - TIP).

Điều 2. Khuyến nghị cơ quan, tổ chức nghiên cứu, phát triển, lựa chọn, sử dụng sản phẩm TIP đáp ứng các yêu cầu kỹ thuật cơ bản theo Điều 1 Quyết định này.

Điều 3. Cục An toàn thông tin chủ trì, phối hợp với các cơ quan, tổ chức liên quan hướng dẫn việc áp dụng các yêu cầu trong Yêu cầu kỹ thuật cơ bản đối với sản phẩm TIP tại Điều 1 Quyết định này.

Điều 4. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 5. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin, Thủ trưởng các đơn vị thuộc Bộ, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 5;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Cổng thông tin điện tử của Bộ;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng

YÊU CẦU KỸ THUẬT CƠ BẢN ĐỐI VỚI SẢN PHẨM NỀN TẢNG TRI THỨC MỐI ĐE DỌA AN TOÀN THÔNG TIN

(Kèm theo Quyết định số 1517/QĐ-BTTTT ngày 06 tháng 10 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. THÔNG TIN CHUNG

1. Phạm vi áp dụng

Tài liệu này mô tả các yêu cầu kỹ thuật cơ bản đối với sản phẩm Nền tảng tri thức mối đe dọa an toàn thông tin (Threat Intelligence Platform - TIP). Tài liệu bao gồm các nhóm yêu cầu là Yêu cầu về tài liệu, Yêu cầu về quản trị hệ thống, Yêu cầu về kiểm soát lỗi, Yêu cầu về log, Yêu cầu về hiệu năng xử lý, Yêu cầu về chức năng tự bảo vệ, Yêu cầu về chức năng thống kê xu hướng và cảnh báo mối đe dọa.

2. Đối tượng áp dụng

Các cơ quan, tổ chức có liên quan đến hoạt động nghiên cứu, phát triển; đánh giá, lựa chọn sản phẩm TIP khi đưa vào sử dụng trong các hệ thống thông tin.

3. Khái niệm và thuật ngữ

Trong tài liệu này các khái niệm và thuật ngữ được hiểu như sau:

3.1. Nhật ký hệ thống (log)

Sự kiện an toàn thông tin được hệ thống ghi lại, liên quan đến trạng thái hoạt động, thông báo, cảnh báo, sự cố, cuộc tấn công, thông tin về các mối đe dọa thu thập được và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

3.2. Thời gian duy trì phiên kết nối (session timeout)

Khoảng thời gian được thiết lập để cho phép hệ thống hủy phiên kết nối đối với một máy khách, nếu trong khoảng thời gian này mà hệ thống không nhận được yêu cầu mới từ máy khách đó.

II. YÊU CẦU CƠ BẢN

1. Yêu cầu về tài liệu

TIP có tài liệu bao gồm các nội dung sau:

a) Hướng dẫn triển khai và thiết lập cấu hình;

b) Hướng dẫn sử dụng và quản trị.

2. Yêu cầu về quản trị hệ thống

2.1. Quản lý vận hành

TIP cho phép quản lý vận hành đáp ứng các yêu cầu sau:

a) Cho phép thiết lập, thay đổi, áp dụng và hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng;

b) Cho phép cấu hình thời gian hệ thống;

c) Cho phép cấu hình thời gian duy trì phiên kết nối;

d) Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa (ví dụ: giới hạn địa chỉ IP, giới hạn số phiên kết nối quản trị từ xa đồng thời,...);

đ) Cho phép đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực;

e) Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại;

g) Cho phép xóa log;

h) Cho phép xem thời gian hệ thống chạy tính từ lần khởi động gần nhất.

2.2. Quản trị từ xa

TIP cho phép quản trị từ xa an toàn đáp ứng các yêu cầu sau:

a) Sử dụng giao thức có mã hóa như TLS hoặc tương đương;

b) Tự động đăng xuất tài khoản và hủy bỏ phiên kết nối quản trị từ xa khi hết thời gian duy trì phiên kết nối.

2.3. Quản lý xác thực và phân quyền

TIP cho phép quản lý cấu hình tài khoản xác thực và phân quyền người dùng đáp ứng các yêu cầu sau:

a) Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu, trong đó, quản trị viên có thể thiết lập và thay đổi được độ phức tạp của mật khẩu;

b) Hỗ trợ phân nhóm tài khoản tối thiểu theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm.

2.4. Quản lý báo cáo

TIP cho phép quản lý báo cáo thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo;

b) Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước;

c) Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo;

d) Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML;

đ) Cho phép tải về tệp tin báo cáo đã được xuất ra.

2.5. Chia sẻ dữ liệu

a) TIP cho phép kết nối với các loại hệ thống sau để chia sẻ dữ liệu:

i) Các giải pháp và nền tảng khác loại (tối thiểu là SIEM);

ii) Hệ thống TIP khác được phát triển bởi chính nhà sản xuất.

b) TIP cho phép chia sẻ dữ liệu log thông tin mối đe dọa theo tối thiểu 01 trong các cách thức sau:

i) Chuẩn quốc tế STIX/TAXII;

ii) Đường dẫn URL (API).

3. Yêu cầu về kiểm soát lỗi

3.1. Bảo vệ cấu hình

Trong trường hợp TIP phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), TIP đảm bảo các loại cấu hình sau mà đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp:

a) Cấu hình hệ thống;

b) Cấu hình quản trị từ xa;

c) Cấu hình tài khoản xác thực và phân quyền người dùng.

3.2. Bảo vệ dữ liệu log

Trong trường hợp TIP phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), TIP đảm bảo dữ liệu log đã được lưu lại phải không bị thay đổi trong lần khởi động kế tiếp.

3.3. Đồng bộ thời gian hệ thống

Trong trường hợp TIP phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), TIP đảm bảo thời gian hệ thống phải được đồng bộ tự động đến thời

điểm hiện tại.

4. Yêu cầu về log

4.1. Log quản trị hệ thống

a) TIP cho phép ghi log quản trị hệ thống về các loại sự kiện sau:

i) Đăng nhập, đăng xuất tài khoản;

ii) Xác thực trước khi cho phép truy cập vào tài nguyên, sử dụng chức năng của hệ thống;

iii) Áp dụng, hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng;

iv) Kích hoạt lệnh khởi động lại, tắt hệ thống;

v) Thay đổi thủ công thời gian hệ thống.

b) TIP cho phép ghi log quản trị hệ thống có các trường thông tin sau:

i) Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây);

ii) Địa chỉ IP hoặc định danh của máy trạm;

iii) Định danh của tác nhân (ví dụ: tài khoản người dùng, tên hệ thống,...);

iv) Thông tin về hành vi thực hiện (ví dụ: đăng nhập, đăng xuất, thêm, sửa, xóa, cập nhật, hoàn tác,...);

v) Kết quả thực hiện hành vi (thành công hoặc thất bại);

vi) Lý do giải trình đối với hành vi thất bại (ví dụ: không tìm thấy tài nguyên, không đủ quyền truy cập,...).

4.2. Log thông tin mối đe dọa

a) TIP cho phép thu thập và lưu trữ log thông tin mối đe dọa từ phía nhà cung cấp sản phẩm TIP.

b) TIP cho phép thu thập và lưu trữ log thông tin mối đe dọa có các loại thông tin sau:

i) Mô tả tổng quan mối đe dọa;

ii) Mức độ nguy hiểm của mối đe dọa (severity level);

iii) Mức độ tin cậy về dữ liệu của mối đe dọa (confidence level);

iv) Các phân nhóm được gán cho mối đe dọa;

v) Các thuộc tính mô tả chi tiết mối đe dọa.

b) TIP cho phép thu thập log thông tin mối đe dọa qua hai cách thức thủ công và tự động.

4.3. Log cảnh báo

TIP cho phép ghi log cảnh báo được sinh ra bởi việc thực thi các thiết lập cảnh báo mối đe dọa.

4.4. Định dạng log

TIP cho phép chuẩn hóa log theo tối thiểu 01 định dạng đã được định nghĩa trước để truyền dữ liệu log cho các phần mềm quản lý, phân tích, điều tra log.

4.5. Quản lý log

TIP cho phép quản lý log đáp ứng các yêu cầu sau:

a) Cho phép thiết lập và cấu hình các cài đặt liên quan đến lưu trữ và hủy bỏ log (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ,...);

b) Cho phép tìm kiếm log theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có);

c) Cho phép tìm kiếm log thông tin mối đe dọa theo thời gian, giá trị băm của mã độc và phân nhóm;

d) Cho phép truy xuất log thông tin mối đe dọa thông qua cảnh báo;

đ) Cho phép xuất dữ liệu log ra để phục vụ cho việc tích hợp các dữ liệu này vào TIP khác hoặc giải pháp khác về quản lý, phân tích, điều tra log.

4.6. Phân nhóm log thông tin mối đe dọa

TIP cho phép phân loại và gán nhãn tên phân nhóm cho log thông tin mối đe dọa theo các phân nhóm sau phục vụ cho mục đích tìm kiếm:

a) Điểm yếu, lỗ hổng an toàn thông tin đã được công bố;

b) Họ mã độc;

c) Kỹ thuật tấn công;

d) Chiến dịch tấn công;

đ) Mục đích tấn công;

e) Loại đối tượng, tổ chức bị tấn công;

g) Đối tượng, tổ chức thực hiện tấn công;

h) Tên miền, địa chỉ IP của khách hàng có kết nối đến cơ sở hạ tầng của đối tượng, tổ chức thực hiện tấn công;

i) Điểm yếu, lỗ hổng an toàn thông tin đối với hệ thống của khách hàng.

5. Yêu cầu về hiệu năng xử lý

TIP được triển khai thỏa mãn cấu hình tối thiểu theo hướng dẫn cài đặt và thiết lập cấu hình của nhà sản xuất phải đảm bảo đáp ứng các yêu cầu sau:

a) TIP đảm bảo rằng độ trễ thời gian tìm kiếm log với độ phức tạp bất kỳ, có phản hồi trong khoảng thời gian tối đa là 02 phút;

b) Dữ liệu tri thức các mối đe dọa của TIP có tối thiểu 100.000 bản ghi.

6. Yêu cầu về chức năng tự bảo vệ

6.1. Phát hiện và ngăn chặn tấn công hệ thống

TIP có khả năng tự bảo vệ, ngăn chặn các dạng tấn công phổ biến sau vào giao diện ra bên ngoài của hệ thống, bao gồm tối thiểu các dạng sau:

a) SQL Injection;

b) OS Command Injection;

c) XPath Injection;

d) Remote File Inclusion (RFI);

đ) Local File Inclusion (LFI);

e) Cross-Site Scripting (XSS);

g) Cross-Site Request Forgery (CSRF).

6.2. Cập nhật bản vá hệ thống

TIP có chức năng cho phép cập nhật bản vá để xử lý các điểm yếu, lỗ hổng bảo mật.

7. Yêu cầu về chức năng thống kê xu hướng và cảnh báo mối đe dọa

7.1. Thống kê xu hướng mối đe dọa trên thế giới

TIP có chức năng cho phép thống kê các mối đe dọa trên thế giới thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép thống kê xu hướng mối đe dọa dưới dạng biểu đồ;

b) Cho phép tìm kiếm dữ liệu xu hướng mối đe dọa theo thời gian (tối thiểu theo 04 mức: năm, quý, tháng, ngày).

7.2. Quản lý thiết lập cảnh báo

TIP có chức năng cho phép quản lý thiết lập cảnh báo mối đe dọa đến người dùng đáp ứng các yêu cầu sau:

a) Cho phép nhận cảnh báo theo các phân nhóm được mô tả ở 4.6;

b) Cho phép thiết lập thời gian nhận cảnh báo;

c) Cho phép tải nội dung cảnh báo dưới dạng tập tin;

d) Cho phép hiển thị nội dung cảnh báo trên giao diện đồ họa về quản lý cảnh báo;

đ) Cho phép nhận cảnh báo qua phương thức gửi thư điện tử hoặc tin nhắn SMS.